

# Using certificates as authentication method for VPN connections between Netgear ProSafe Routers and the ProSafe VPN Client

This document describes how to use certificates as an authentication method when establishing a VPN Client-to-Box connection.



Business Network Network address: 192.168.10.0

## **Preliminary notes:**

If for your particular deployment you are not using an external CA (Certificate Authority) you will need to create your own CA. Some alternatives on how to achieve this are outlined below, but they are not exclusive to other methods:

- 1- OpenSSL: http://www.openssl.org,
- 2- SimpleCA: <u>http://www.vpnc.org/SimpleCA/</u>
- 3- Microsoft's IIS

For purpose of this document we used:

- 1- OpenSSL which could be downloaded from the following link: http://www.slproweb.com/products/Win32OpenSSL.html
- 2- Additionally you will need to install the Perl interpreter. We used ActivePerl which can be downloaded from here: <u>http://www.activestate.com/Products/activeperl/index.mhtml</u>

## Creating your own Certificate Authority with OpenSSL

- 1- In first step you need to create your own CA. To do that, follow the instructions documented in here: <u>http://sandbox.rulemaker.net/ngps/m2/howto.ca.html</u>
- 2- Netgear doesn't support ST relative distinguish name so please edit the openssl.cfg (in the original location and in your new CA folder) to avoid using this parameter.
- 3- From the guide linked above, you need only to execute all the commands up to step 4. The certificate request step and beyond will be handled by the router.
- 4- Next please generate Self Certificate Request specifying the following parameters:

⊯ Generate Self Certificate Request	Phelp
Name: first Subject: CN=router1 Hash Algorithm: MD5 X Signature Algorithm: RSA S Signature Key Length: FORE X IP Address (Optional): 0 40 40 40 Domain Name (Optional): C E-mail Address (Optional): C Senerate	<ol> <li>Name: first</li> <li>Subject: CN=router1</li> <li>Hash Algorithm: MD5</li> <li>Signature Algorithm: RSA</li> <li>Signature Key Length: 1024</li> <li>Click on Generate</li> </ol>

5- Click on: "View" for generated certificate request to check its values:





6- Sign your certificate request using your newly created CA:

Openssl x509 -req -days 365 -in router1.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial - out router1.crt

router1.csr - generated self certificate request (router), cacert.crt - CA certification, cakey.pem - CA keys, router1.crt - signed certificate (router).

7- Load CA certificate: "cacert.crt" and your signed certificate: "router1.crt" on your device. They now should display like this:

# ·	Trusted Certificates (CA Certificate)		?help
	CA Identity (Subject Name)	Issuer Name	Expiry Time
			Dec 9
	CHECK CHECK CHECK CHECK CHECK CHECK		17:22:42
	CN-Supervisor/email/codiess-supervisor@orange.pr	CN-Supervisor, email@dress-supervisor@orange.pr	2011 GMT

 Activ	e Self Certi	ficates		?help
Name	Subject Name	Serial Number	Issuer Name	Expiry Time
first	CN=router1	89:65:46:12:fb:∍3:0f:80⊡	C=PL, O=Orange PL, OU=IT Support, CN=Supervisor/emailAddress=supervisor@orange.pl	Dec 16 13:00:50 2009 GMT

8- Reboot your router.

9- Next – generate certificate request using Certificate Manager which is built-in functionality of Netgear's ProSafe VPN Client following these steps:

My Certificates   Root CA Certificates   Trust Policy   CA Certificates   RA Certificates   CRLs   Requests   About	
Personal certificates identify you to people and security gateways you communicate with. <b>NETGEAR</b>	
Show certificates for: C users C this computer C all	
View Verify Delete Export	First, click on Request Certificate.
Request Cettificate	
There aren't any CAs configured for online certificate enrollment. Please go to the "CA Certificates" page and retrieve a CA certificate. Do you wish to make a file-based request instead? Yes No	Then, click on 'Yes' when you get the file- based request prompt.
🚺 File-based Certificate Request - NETGEAR ProSafe VPN Client	1
Generate a Private/Public key pair and request a personal certificate.	
Subject Name F Enter Subject Name in LDAP format Subject name in LDAP format	
Subject Alternate Name Email: Domain Name: IP Address: "Required Fields	For last, input the settings like instructed in the screenshot.
Request File Filename: C:\Temp\CettReq.teg Browse Cancel	

**Note:** Do not change file extension in client software. Change the whole filename after creating a certificate request instead.

- 10- Rename the generated certificate request from:"CertReq.req" to "client1.csr".
- 11- Sign your certificate request using your newly created CA:

openssl x509 -req -days 365 -in client1.csr -CA cacert.crt -CAkey cakey.pem -CAcreateserial -out client1.crt

client1.csr – generated self certificate request (client), cacert.crt – CA certification, cakey.pem – CA keys, client1.crt – signed certificate (client).

- 12- Install CA certificate: "cacert.crt" in your system. If you are using Microsoft Windows just select: "Install" from files' context menu.
- 13- Load your signed certificate using the Certificate Manager:

Import Person	al Certificate	
	Import Type	
CSP:	IRE Cryptographic Service Provider	Ţ
Certificate File:	F:\FVS\client1.crt	Browse
Key File:	C:\DOCUME~1\Support\LOCALS~1\Temp\Ke	Browse
Password:		
	Import	

14- Create a new VPN connection according to these steps:

N Security Policy Editor - NETGEAR ProS	afe VPN Client
File Edit Options Help	
File Edit Options Help Network Security Policy Microsoft Prec VPN Microsoft Prec VPN My Connections G My Identity G My I	Connection Security Secure Non-secure Block Remote Party Identity and Addressing D. Lino (Dischart)
	Subnet: 19216810.0 Mask: 255 255.0 Protocol All Pot All V V Use Secure Gateway Tunnel ID Type Distinguished Name Gateway IP Address C Edit Name 128.121

First, input your own details in the same way that is instructed here and click on Edit Name.

E	dit Distinguishe	d Name	×
	- Subject Information	n	
		Enter Subject Name in LDAP format	
	Subject name in LDAP format:	CN=router1	
		One LDAP name component per line	
		OK Cancel	

Verify your settings are input correctly in this screen and click on OK.

N Security Policy Editor - NETGEAR ProS	afe VPN Client 📃 🗖 🗙
N Security Policy Editor - NETGEAR ProS File Edit Options Help Network Security Policy Microsoft Psec VPN → My Connections ↓ Let ↓ Let ↓ Security Policy ↓ Security Poli	Afe VPN Client       NETGEAR       My Identity       Select Certificate       Unclient's Orange PL IT Support ID       UD Type       Port       Distinguished Name       CN=client1       Secure Interface Configuration       Virtual Adapter       Required
	Internal Network IP Address 0.0.0.0 Internet Interface Name Arry IP Addr Arry IP Addr Arry

Select the correct certificate, leave the ID Type as Distinguished Name.

Virtual adapter should be specified as: "Required" to allow using of virtual adapter interface on the client.

lie Edit Options Help Network Security Policy → Microsoft (Pase VPN → My Connections → My Lornetions → My Identity → G My Identity →	Security Policy Select Phase 1 Negotiation Mode Main Mode Aggressive Mode Use Manual Keys IV Enable Perfect Forward Secrecy (PFS) PFS Key Group Diffie Helman Group 2 I
---	---

#### In the Security Policy section, verify your settings match those in this screenshot.

File Edit Options Help	
Network Security Policy Microsoft I See VPN My Identity Security Policy Security Policy Security Policy Key Exchange (Phase 1) Proposal 1 Where Connections	Authentication Method and Algorithms Authentication Method RSA Signature:

### For the "Proposal 1" of the Authentication phase (Phase 1), the Authentication Method should be RSA Signatures.

Naharah Securita Delina	NETGEAR 😽
Herosoft Peec VP     Moreotions     Moreotions     Moreotions     Moreotions     Moreotions     Moreotion(Phase 1)     Proposal 1     Proproposal 1     Proposal 1     Proposal 1	IPSec Protocols Seconds KBytes SA Life Unspecified ▼ Compression None ▼ ▼ Encepsulation Protocol (ESP) Encrypt Alg Triple DES ▼ Hash Alg SHA-1 ▼ Encepsulation Tunnel ▼ ■ Authentication Protocol (AH) Hash Alg SHA-1 ▼ Encepsulation Tunnel ▼

The Key Exchange Proposal should be correct by default, but check it to make sure it matches the settings on the screenshot nonetheless.

- 1. Create IKE and VPN policies on your router using VPN Wizard.
- 2. Delete the VPN Policy, leaving the IKE policy.
- 3. Create new record for Mode Config in the following way:

# Client Pool		2 help
	Record Name: testm	
First Pool:	Starting IP 192 .168 .20 .1 Ending IP 192 .168 .20 .100	
Second Pool:	Starting IP 0 +0 +0 = Ending IP 0 +0 +0	
Third Pool:	Starting IP 0 .0 .0 .0 Ending IP 0 .0 .0 .0	
WINS Server:	Primary 0 •0 •0 •0 Secondary 0 •0 •0	
DNS Server:	Primary 0 0 0 0 Secondary 0 0 0	
# Traffic Tunnel Secur	ity Level	
		Oneip
	PFS Key Group: DH Group 2 (1024 bit)	() Help
	PFS Key Group: DH Group 2 (1024 bit) V SA Lifetime: 3600 Seconds V	Uneip
	PFS Key Group: DH Group 2 (1024 bit) V SA Lifetime: 3600 Seconds V Encryption Algorithm: 3DES V	(Jueip
	PFS Key Group: DH Group 2 (1024 bit) V SA Lifetime: 3600 Seconds V Encryption Algorithm: 3DES V Integrity Algorithm: SHA-1 V	. Micib
<u> </u>	V PFS Key Group: DH Group 2 (1024 bit) V SA Lifetime: 3600 Seconds V Encryption Algorithm: 3DES V Integrity Algorithm: SHA-1 V Local IP Address: 192 168 10 0	(Mielb
<u>- 110110 (0110) Seco</u>	<ul> <li>✓ PFS Key Group: DH Group 2 (1024 bit) ▼</li> <li>SA Lifetime: 3600 Seconds ▼</li> <li>Encryption Algorithm: 3DES ▼</li> <li>Integrity Algorithm: SHA-1 ▼</li> <li>Local IP Address: 192 ,168 ,10 ,0</li> <li>Local Subnet Mask: 255 ,255 ,0</li> </ul>	C. Leik
	<ul> <li>♥ PFS Key Group: DH Group 2 (1024 bit) ♥</li> <li>SA Lifetime: 3600 Seconds ♥</li> <li>Encryption Algorithm: 3DES ♥</li> <li>Integrity Algorithm: SHA-1 ♥</li> <li>Local IP Address: 192 168 10 0</li> <li>Local Subnet Mask: 255 255 255 0</li> </ul>	

**Note:** IP address ranges defined in: First, Second and Third Pool should be different then router's own LAN IP address range.

4. Modify your IKE Policy according to the following settings:

III Mode Config Record	elp 🗰 General 📀 help
Do you want to use Mode Config Record? Yes C No Select Mode Config Record: testm view selected	Policy Name: test Direction / Type: Responder 💌 Exchange Mode: Aggressive 💌
Identifier Type: DER ASN1 DN V Identifier: CN=router1	elp II Remote Ohelp Identifier Type : DER ASN1 DN I Identifier: CN=client1
IKE SA Parameters	() help
Encryption Algorithm: 3DES Authentication Algorithm: SHA-1 Authentication Method: C Pre-shared key RSA-Signature Pre-shared key: (Key Length 8 - 49 Char) Diffie-Hellman (DH) Group: Group 2 (1024 bit) SA-Lifetime (sec): 28800 Enable Dead Peer Detection: C Yes No Detection Period: 10 (Seconds) Reconnect after failure count: 3	
Extended Authentication	elp
XAUTH Configuration None Edge Device IPSec Host Apply	Authentication Type: User Database 🗾 Username: Password: Reset